Vendors must have an active, approved master contract under the SITE program and be approved in the category or categories listed in the RFO document in order to respond to and RFO. Vendor is responsible for reading all addenda associated with the RFO.

IT Professional Technical Services

SITE Program

T#:14ATM

Request for Offers (RFO) For Technology Services Issued By

Minnesota Office of Secretary of State

Project Title: *Web Vulnerability Assessment*

Category: *Security*

Business Need The Minnesota Office of Secretary of State (OSS) is seeking Professional/Technical Services to perform web application security testing to assess the vulnerability of all of our public facing websites, systems and networks from an access point external to our system. Services should include discovery scans and tests to determine if there are currently unknown available points of access to our system. Testing should be performed using both automated and manual techniques. The purpose of this testing is to identify vulnerabilities that could pose a threat to our technology assets with particular attention to vulnerabilities that would temporarily disrupt access to our website or databases, would allow for access to or manipulation of non public data, or result in unauthorized data being displayed on our public web pages. The OSS website is a critical mechanism that provides information to citizens, business owners, election officials and others. The elections systems are of particular concern this year. With the high visibility of the upcoming 2016 presidential election and the importance of the data provided to the media on election night, it is incumbent on OSS to ensure that election data is as safe as possible and available in a timely manner on election night. The OSS environment consists of a number of applications containing multiple input forms. The applications are supported by multiple hosts and URLs. Detailed information regarding each application will be provided to the selected vendor once a contract and appropriate confidentiality agreements are in place. The assessment and testing efforts will be prioritized with emphasis given to systems used to support the upcoming election on November 8. A summary of those applications is provided here for reference: OSS External Website: Content management-based system. Statewide Voter Registration System (SVRS): Manages voter registrations, precinct and district management, election roster generation, county absentee ballot and the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) administration, and voting history. On-Line voter registration: Allows Minnesota citizens to register on-line to vote. Election Reporting System (ERS): Manages all election activities at the precinct level, including candidate filing, data exports for ballot and voting equipment programming, election results reporting, web-reporting, results file generation for media, and election administration and results reports for all jurisdictions in the election.

Poll Finder: Provides public look up by address range of polling place for any precinct in the State, using a combination of SVRS and ERS data. It provides information on upcoming elections, offices and candidates on the precinct ballot and districts.

Caucus Finder: Provides public look up by address range of precinct caucus location for any precincts or party in the State using location information submitted by political parties.

Minnesota Business and Liens PORTAL (MBLS Portal): Used for a wide variety of services such as corporate filings, business registrations, tax liens, etc. The current implementation includes several different applications and platforms.

Other Applications: notary, official documents, commissions and appointments.

In addition to the assessment of the aforementioned sites and applications, an internal penetration test shall be carried out with the perspective of a malicious insider such as a rogue employee or contractor acting within OSS internal network. The test will include an attempt to enumerate as much information as possible about the environment (such as identifying all logical assets that belong to OSS). This may be accomplished with passive traffic analysis, DNS and LDAP queries, social engineering and other techniques. OSS has two office locations 60 Empire Drive and 100 Martin Luther King Blvd. Both locations need to be assessed for network, social and physical security vulnerabilities.

This Statement of Work does not include code review or remediation of any vulnerabilities that are found.

Project Deliverables

The project will include the following tasks:

- Vulnerability scan (automated) of OSS websites and all public facing applications.
- Manual testing of OSS websites and all external applications for vulnerability assuming a motivated attacker or better.
- Internal vulnerability assessment (manual and automated) of the OSS environment in order to discover any vulnerability not associated with known applications, network, servers, etc.
- Identification and confirmation of false positives from the vulnerability scan.

Deliverables:

1. Completed web application security test performed according to the plan agreed upon by OSS and the selected vendor.
2. Final report including the following:
    a. Executive summary
    b. Identification of potential exposures and vulnerabilities for the network; websites and web applications; internal, external, and physical security. Report should identify application-specific vulnerabilities in addition to overall network vulnerabilities.
    c. Severity of each vulnerability.
    d. How each vulnerability was found – manual or automated and if automated what tool was used.
    e. Analysis of each vulnerability found as a result of scanning using an automated tool to ensure it is not a false positive.
    f. Recommendations for remediation of each vulnerability including prioritization of proposed actions, and approximate costs if known.
    g. Recommendations for enhancing the security of the entire network.
3. Up to 16 hours (clock time) on site at OSS of meetings for planning, questions, and the reviewing of findings.

Project Milestones and Schedule

- Project Start Date August 29, 2016
- End Date No later than October 14th 2016

Project Environment

Work for this project will be performed onsite and offsite. Assessment report reviews will be performed onsite at the Secretary of State's office in Saint Paul, MN during scheduled meetings.

Project Requirements

The project is expected to be completed onsite and off-site, after necessary system data is provided to the vendor. Once completed, the resulting report and any associated data are to be delivered to OSS.

Any testing done as a result of this SOW must be discovery only – no changes may be made to OSS data. No data trophies are necessary to prove penetration.

Training of OSS staff can be done in person or via an online vehicle, such as Webex.

Any testing done that may impact the performance of OSS systems will be completed after normal business hours, and scheduled with OSS management.

Responsibilities Expected of the Selected Vendor

Corporate references, corporate experience and time in business will also be included in the evaluation process, as shown in the "RFO Evaluation Process" section.

Mandatory Qualifications (to be initially scored as pass/fail. Thereafter, vendors that meet the Mandatory Qualifications will be scored in part on the extent to which the vendor exceeds these mandatory minimums. See RFO Evaluation Process below.)

- Vendor possesses at least six years' experience in risk assessment or network scanning. Vendor is expected to enumerate experience with web site assessments, tools utilized, and types of web-applications assessed, and the architectures of those applications (such as ASP.NET, Java, etc…).
- Vendor will provide documentation of their formal testing procedures for common vulnerabilities such as OWASP and social engineering.
- Vendor will provide documentation of their procedures ensuring that any sensitive or confidential data collected during the testing process is adequately protected.
- Vendor has completed at least 5 similar assessments in the past.

Desired Skills

Vendor holds an industry recognized IT security certification (ASV) and / or deploys certified individuals to the project (CISSP, etc…).

Process Schedule

Process Milestone	Due Date
Deadline for Questions	08/03/2016, 3PM CST
Anticipated Posted Response to Question	08/05/2016, 3PM CST
Proposals due	08/12/2016, 3PM CST
Anticipated proposal evaluation begins	08/15/2016, 8AM CST
Anticipated proposal evaluation & decision	08/19/2016, 3PM CST

Questions

Any questions regarding this Request for Offers should be submitted via e-mail according to the date and time listed in the process schedule to:

Name: Dan Auger
Organization: Minnesota Office of Secretary of State
Email Address: dan.auger@state.mn.us

Questions and answers will be posted via an addendum to the RFO on the Office of MN.IT Services website (http://mn.gov/buyit/14atm/rfo/active.html) according to the process schedule above.

Other persons ARE NOT authorized to discuss this RFO or its requirements with anyone throughout the selection process and responders should not rely on information obtained from non-authorized individuals. If it is discovered a Responder contacted other State staff other than the individual above, the responder's proposal may be removed from further consideration.

RFO Evaluation Process

- **Evaluation Process**. Each vendor will be evaluated based on the following criteria:
  - Proposed application security test plan – thoroughness and applicability
  - Corporate experience with similar projects
  - Corporate information, security certifications held by staff that would be assigned to this project and references
  - Cost
- **Scoring/weighting**
  - Thoroughness and applicability of proposed application security test plan (35%)
  - Corporate experience with similar web site assessments (25%)
  - Corporate information, security certifications held by staff that would be assigned to this project and references (5%)
  - Corporate references (5%)
  - Cost (30%). Based on the cost to perform a single complete scan on the applications listed.

This Request for Offers does not obligate the state to award a work order or complete the assignment, and the state reserves the right to cancel the solicitation if it is considered to be in its best interest. The Organization reserves the right to reject any and all proposals.

Submission Format

The proposal should be assembled as follows:

1. **Cover Page**
   Master Contractor Name
   Master Contractor Address
   Contact Name for Master Contractor
   Contact Name's direct phone/cell phone (if applicable)
   Contact Name's email address

2. **Project Plan**
   Include the following elements (not in a particular order):
   - Description of the methodology used
   - Milestones and high level tasks, including approximate duration of work
   - Introduction or brief "SOW response letter" explaining understanding / scope of project
   - Corporate overview, history, summary experience & skills
   - Proposed high level web application security test plan and approach for OSS systems
   - Experience listing of similar assessments, including tools used and system architecture tested. Minimum of 5 examples.
   - Sample report from a similar assessment with any sensitive information removed or blocked out
   - Corporate References where similar work has been performed (3)

3. **Resumes of staff that would be assigned to this project.**

4. **Cost Proposal**
   Include a separate document labeled "Cost Proposal" which outlines total cost of the project. This includes each resource being submitted and their corresponding proposed hourly rate. Should also include any non-resource line items (example: if the cost of a scan or product is not tied to resource hours).

5. **Conflict of interest statement as it relates to this project**

6. **Additional Statement and forms:**

   1. Affirmative Action Certificate of Compliance (if over $100,000, including extension options) http://www.mmd.admin.state.mn.us/doc/affaction.doc
   2. Equal Pay Certificate Form (if proposals exceeds $500,000, including extension options) http://www.mmd.admin.state.mn.us/doc/equalpaycertificate.doc
   3. Affidavit of non-collusion http://www.mmd.admin.state.mn.us/doc/noncollusion-2.doc
   4. Certification Regarding Lobbying (if over $100,000, including extension options) http://www.mmd.admin.state.mn.us/doc/lobbying.doc

The STATE reserves the right to determine if further information is needed to better understand the information presented. This may include a request for a presentation.

Proposal Submission Instructions

- Vendor is limited to one proposal submission for this project.
- Response Information: The resume and required forms must be transmitted via e-mail to:
  Bob.Cross@state.mn.us
  Email subject line must read: Vulnerability assessment response
- Submissions are due according to the process schedule previously listed.
- **A copy of the response must also be sent to MNIT.SITE@state.mn.us for vendor performance tracking.**
- **You must submit an email with your response or email notification that you will not respond to MNIT.SITE@state.mn.us. Failure to do either of these tasks will count against your program activity and may result in removal from the program.**

General Requirements

Proposal Contents

By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of this work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Liability

Indemnification
In the performance of this contract by Contractor, or Contractor's agents or employees, the contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:
1) Intentional, willful, or negligent acts or omissions; or
2) Actions that give rise to strict liability; or

3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

Disposition of Responses

All materials submitted in response to this RFO will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this RFO that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this RFO, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.

Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor's objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage. The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration's Materials Management Division ("MMD") which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve the State's rights.

IT Accessibility Standards

All documents and other work products delivered by the vendor must be accessible in order to conform with the State Accessibility Standard. Information about the Standard can be found at: **http://mn.gov/mnit/programs/policies/accessibility/**.

Preference to Targeted Group and Economically Disadvantaged Business and Individuals

In accordance with Minnesota Rules, part 1230.1810, subpart B and Minnesota Rules, part 1230.1830, certified Targeted Group Businesses and individuals submitting proposals as prime contractors will receive a six percent preference in the evaluation of their proposal, and certified Economically Disadvantaged Businesses and individuals submitting proposals as prime contractors will receive a six percent preference in the evaluation of their proposal. Eligible TG businesses must be currently certified by the Materials Management Division prior to the solicitation opening date and time. For information regarding certification, contact the Materials Management Helpline at 651.296.2600, or you may reach the Helpline by email at mmdhelp.line@state.mn.us. For TTY/TDD communications, contact the Helpline through the Minnesota Relay Services at 1.800.627.3529.

Veteran-Owned Small Business Preference

Unless a greater preference is applicable and allowed by law, in accordance with Minn. Stat. § 16C.16, subd. 6a, the Commissioner of Administration will award a 6% preference in the amount bid on state procurement to certified small businesses that are majority owned and operated by veterans.

A small business qualifies for the veteran-owned preference when it meets one of the following requirements. 1) The business has been certified by the Department of Administration/Materials Management Division as being a veteran-owned or service-disabled veteran-owned small business. 2) The principal place of business is in Minnesota AND the United States Department of Veterans Affairs verifies the business as being a veteran-owned or service-disabled veteran-owned small business under Public Law 109-461 and Code of Federal Regulations, title 38, part 74 (Supported By Documentation). See Minn. Stat. § 16C.19(d).

Statutory requirements and certification must be met by the solicitation response due date and time to be awarded the preference.

Foreign Outsourcing of Work Prohibited

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.

Work Force Certification

For all contracts estimated to be in excess of $100,000, responders are required to complete the Affirmative Action Certificate of Compliance and return it with the response. As required by Minnesota Rule 5000.3600, “It is hereby agreed between the parties that Minnesota Statute § 363A.36 and Minnesota Rule 5000.3400 - 5000.3600 are incorporated into any contract between these parties based upon this specification or any modification of it. A copy of Minnesota Statute § 363A.36 and Minnesota Rule 5000.3400 - 5000.3600 are available upon request from the contracting agency.”

Equal Pay Certification

If the Response to this solicitation could be in excess of $500,000, the Responder must obtain an Equal Pay Certificate from the Minnesota Department of Human Rights (MDHR) or claim an exemption prior to contract execution. A responder is exempt if it has not employed more than 40 full-time employees on any single working day in one state during the previous 12 months. Please contact MDHR with questions at: 651-539-1095 (metro), 1-800-657-3704 (toll free), 711 or 1-800-627-3529 (MN Relay) or at compliance.MDHR@state.mn.us.